



Università degli Studi di Bologna
Corso di Laurea in Ingegneria Informatica

Analisi Requisiti: Sicurezza e Privacy

Ingegneria del Software T

Prof. MARCO PATELLA

Dipartimento di Informatica – Scienza e Ingegneria (DISI)



Outline

- La nuova normativa
- Concetti base
- Analizzare e progettare la sicurezza
- Sistemi critici
- Security Engineering
- Glossario e minacce
- Analisi del rischio
- Specifica dei requisiti di sicurezza
- Security Use Case & Misuse Case

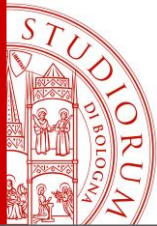


Nuova normativa



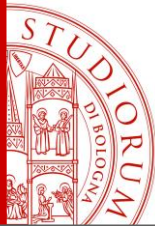
General Data Protection Regulation

- Dal 25/5/2018 sostituisce la Data Protection Directive
- *Obbligo di aderenza (compliance) di un prodotto software che tratti dati personali ai principi della GDPR*
 - *privacy by design & by default* (misure tecniche e organizzative)
 - minimalità, proporzionalità
 - *anonimizzazione, pseudonimizzazione*
 - trasferimento dati fuori dalla EU (occhio al cloud!)
 - adeguatezza delle misure di sicurezza
- *Non è qualcosa che si possa “aggiungere dopo”, a sistema già progettato: va considerato fin dall'inizio*
 - ma non è (solo) un vincolo: è *un'opportunità per creare valore*



Pseudonimizzazione

- **Pseudonimizzazione:**
processo di trattamento dei dati personali in modo tale che i dati non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, sempre che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire la non attribuzione a una persona identificata o identificabile



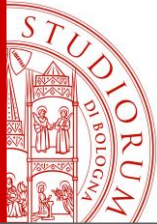
Principi

- I dati personali devono essere:
 - a. trattati in modo lecito, equo e trasparente nei confronti dell'interessato (“**liceità, equità e trasparenza**”)
 - b. raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo non incompatibile con tali finalità
 - c. adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (“**minimizzazione dei dati**”)
 - d. esatti e, se necessario, aggiornati
 - devono essere prese tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati (“**esattezza**”)



Principi

- e. conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati
 - i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente per finalità di archiviazione nel pubblico interesse o per finalità di ricerca scientifica e storica o per finalità statistiche, conformemente all'articolo 83,
- f. *trattati in modo da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali*
(“integrità e riservatezza”)



Articolo 25:

Protezione dei dati fin dalla progettazione e protezione di default

1. Tenuto conto dello stato dell'arte e dei costi di attuazione, nonché della natura, del campo di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi di varia probabilità e gravità per i diritti e le libertà delle persone fisiche costituiti dal trattamento, ***sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso*** il responsabile del trattamento mette in atto ***misure tecniche e organizzative adeguate***, quali la pseudonimizzazione, volte ad attuare i principi di protezione dei dati, quali la minimizzazione, in modo efficace e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati

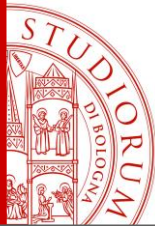


Articolo 25:

Protezione dei dati fin dalla progettazione e protezione di default

2. Il responsabile del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, **di default**, solo i dati personali necessari per ogni specifica finalità del trattamento; ciò vale per la quantità dei dati raccolti, l'estensione del trattamento, il periodo di conservazione e l'accessibilità.

In particolare dette misure garantiscono che, di default, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica



Articolo 32:

Sicurezza del Trattamento

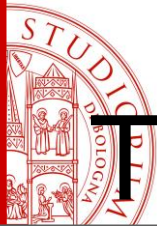
1. Tenuto conto dello stato dell'arte e dei costi di attuazione, nonché della natura, del campo di applicazione, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il responsabile del trattamento e l'incaricato del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono tra l'altro:
 - a. la **pseudonimizzazione** e la **cifratura dei dati personali**;
 - b. la capacità di assicurare la **continua riservatezza**, integrità, disponibilità e resilienza dei sistemi e dei servizi che trattano i dati personali;
 - c. la capacità di **ripristinare tempestivamente la disponibilità** e l'accesso dei dati in caso di incidente fisico o tecnico;
 - d. una procedura per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento



Articolo 32:

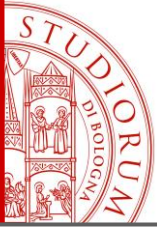
Sicurezza del Trattamento

2. Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo **dei rischi presentati** da trattamenti di dati derivanti in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, memorizzati o comunque trattati
3. L'adesione a un **codice di condotta** approvato di cui all'articolo 40 o a un **meccanismo di certificazione** approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare la conformità ai requisiti di cui al paragrafo 1 del presente articolo

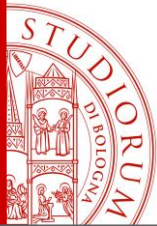


Trasferimento Dati a Paesi Terzi

- Articolo 45:
 - Il trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale è ammesso se la Commissione ha deciso che il paese terzo, o un territorio o uno o più settori specifici all'interno del paese terzo, o l'organizzazione internazionale in questione **garantiscono un livello di protezione adeguato**. In tal caso il trasferimento non necessita di autorizzazioni specifiche.
- Articolo 46:
 - In mancanza di una decisione ai sensi dell'articolo 45, il responsabile del trattamento o l'incaricato del trattamento può trasferire dati personali verso un paese terzo o un'organizzazione internazionale solo se ha offerto garanzie adeguate e a condizione che siano disponibili diritti azionabili degli interessati e mezzi di ricorso effettivi per gli interessati.



Concetti Base



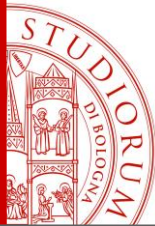
Sicurezza Informatica

- *Salvaguardia dei sistemi informatici* da potenziali rischi e/o violazioni dei dati
- Obiettivo dell'attacco = *contenuto informativo*
- Sicurezza informatica = preoccuparsi di...
 - **impedire l'accesso ad utenti non autorizzati**
 - **regolamentare l'accesso ai diversi soggetti...**
 - **... che potrebbero avere autorizzazioni diverse (relative solo a certe operazioni e non altre)**
- ... per evitare che i dati appartenenti al sistema informatico vengano copiati, modificati o cancellati



Cosa Proteggere

- L'**informazione**...
 - Riservatezza
 - Integrità ed Autenticità
 - Disponibilità
- ... trattata per mezzo di calcolatori e reti
 - Accesso controllato
 - Tre aspetti: *identificazione*, *autenticazione*, *autorizzazione*
 - Funzionamento affidabile



Violazioni

- Le violazioni possono essere molteplici:
 - tentativi non autorizzati di accesso a zone riservate
 - furto di *identità digitale* o di file riservati
 - utilizzo di risorse che l'utente non dovrebbe potere utilizzare
 - ecc.
- La sicurezza informatica si occupa anche di prevenire eventuali *Denial of Service* (DoS)
 - sono attacchi sferrati al sistema con l'obiettivo di rendere inutilizzabili alcune risorse onde danneggiare gli utenti



Fattori Influenti

- Nella scelta delle misure di sicurezza *incidono diverse caratteristiche* dell'informazione e del contesto:
 - Dinamicità
 - Dimensione e tipo di accesso
 - Tempo di vita
 - Costo di generazione
 - Costo in caso di violazione
(di riservatezza, di integrità, di disponibilità)
 - Valore percepito e tipologia di attaccante

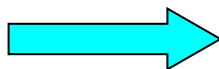
La Catena degli Anelli





Metodi di Protezione

- Legali
- Organizzativi
- Tecnologici
 - Fisici
 - Crittografici
 - Biometrici

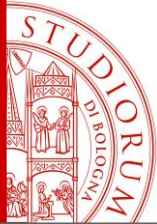


Prevenzione

Rilevazione

Contenimento

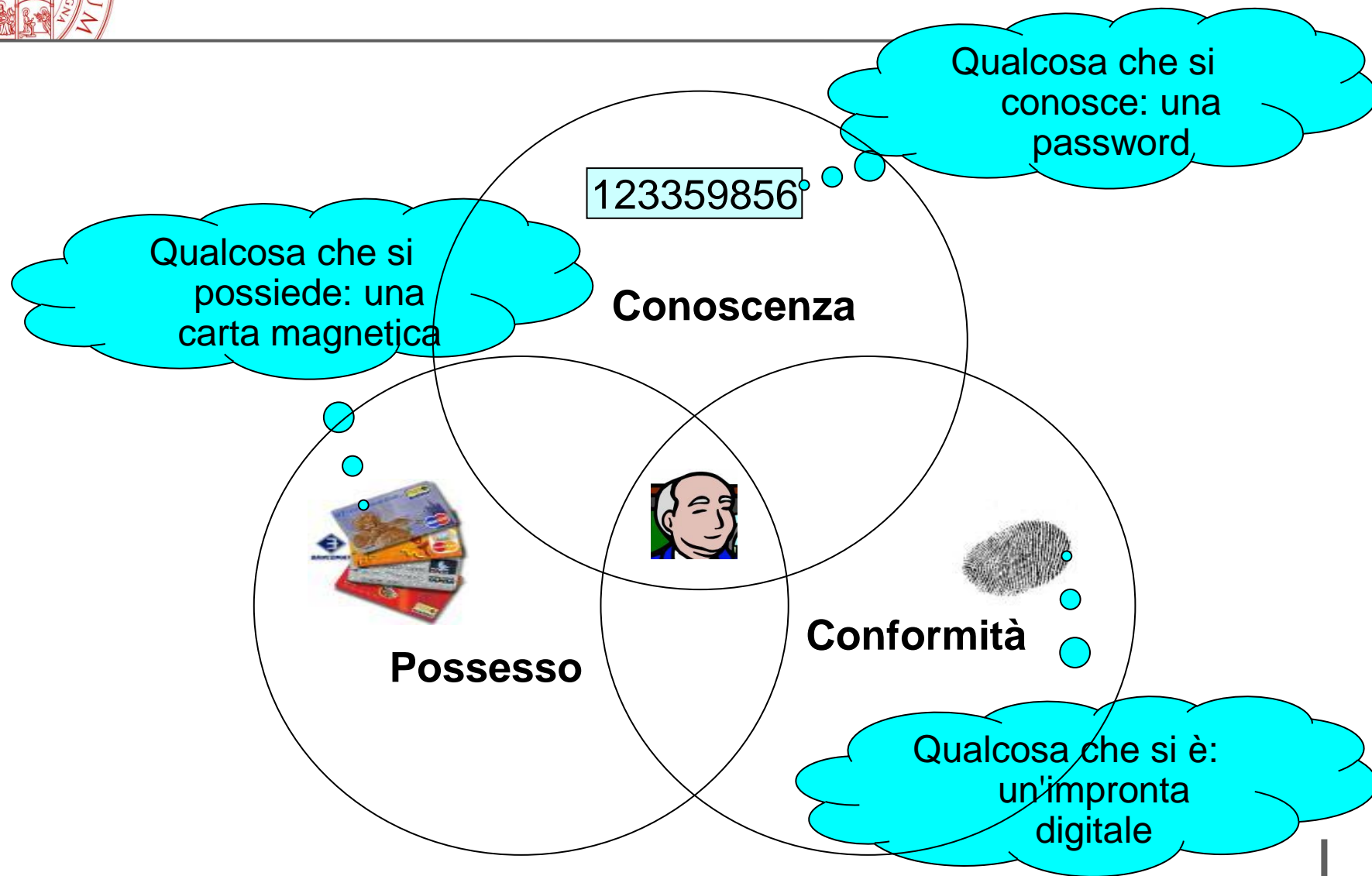
Ripristino

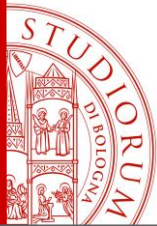


Protezione Fisica

- Essenziale: la vulnerabilità fisica **non sia** la più facilmente attaccabile
- Efficace per i sistemi...
 - criteri che esistono da ben prima dei problemi di sicurezza informatica
- ... e per i dati
 - purché si conosca il comportamento dei sistemi che li trattano (percorsi accessibili, copie temporanee in memoria e su disco, ...)
 - costo di generazione
 - purché si prevedano metodi aggiuntivi per contenere gli effetti delle violazioni fisiche dei sistemi (es. furto)

Autenticazione Forte

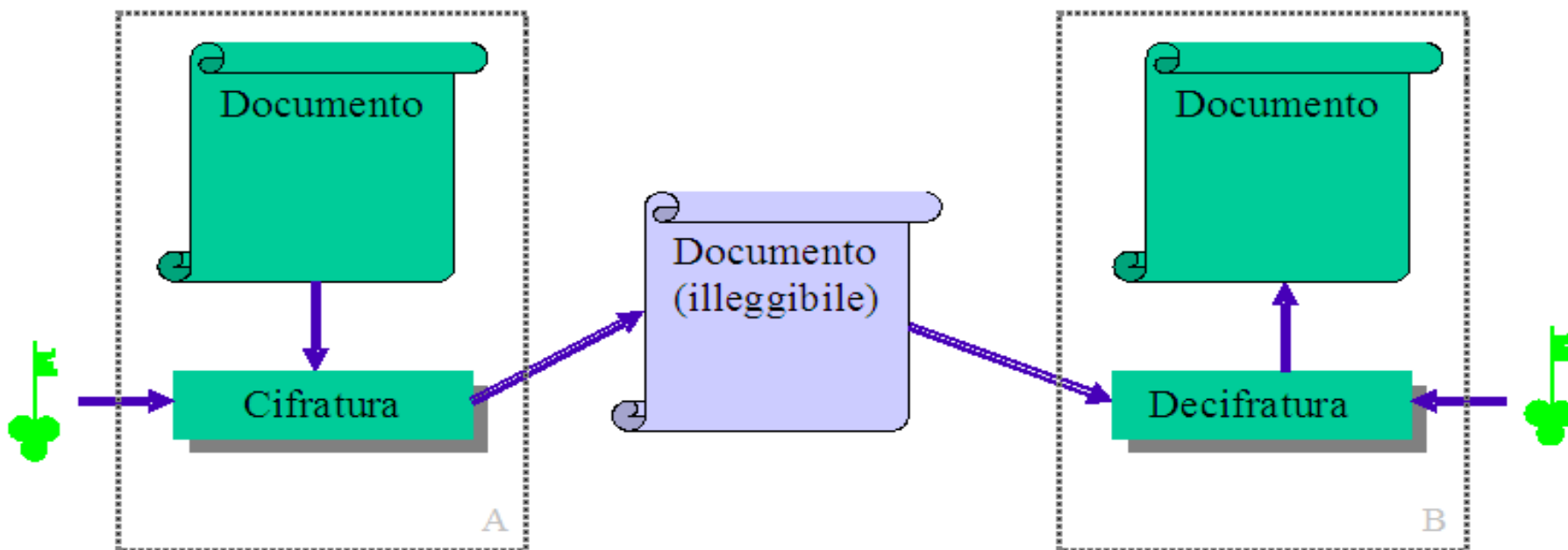




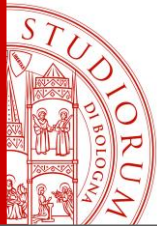
Crittografia

- Crittografia simmetrica
 - garantire riservatezza
 - non identifica né autentica
- Crittografia asimmetrica
 - garantisce riservatezza
 - obiettivo: *identificazione* e quindi autenticazione e paternità
- Infrastrutture per la certificazione della chiave pubblica
 - **Terze parti fidate che possano certificare l'autenticità di una chiave pubblica**

Crittografia Simmetrica



- Classica e moderna, implementata con dispositivi segreti, algoritmi segreti o chiavi segrete
- Tipicamente tecniche derivanti dalla teoria dell'informazione (confusione e diffusione)
- Una singola chiave cifra e decifra



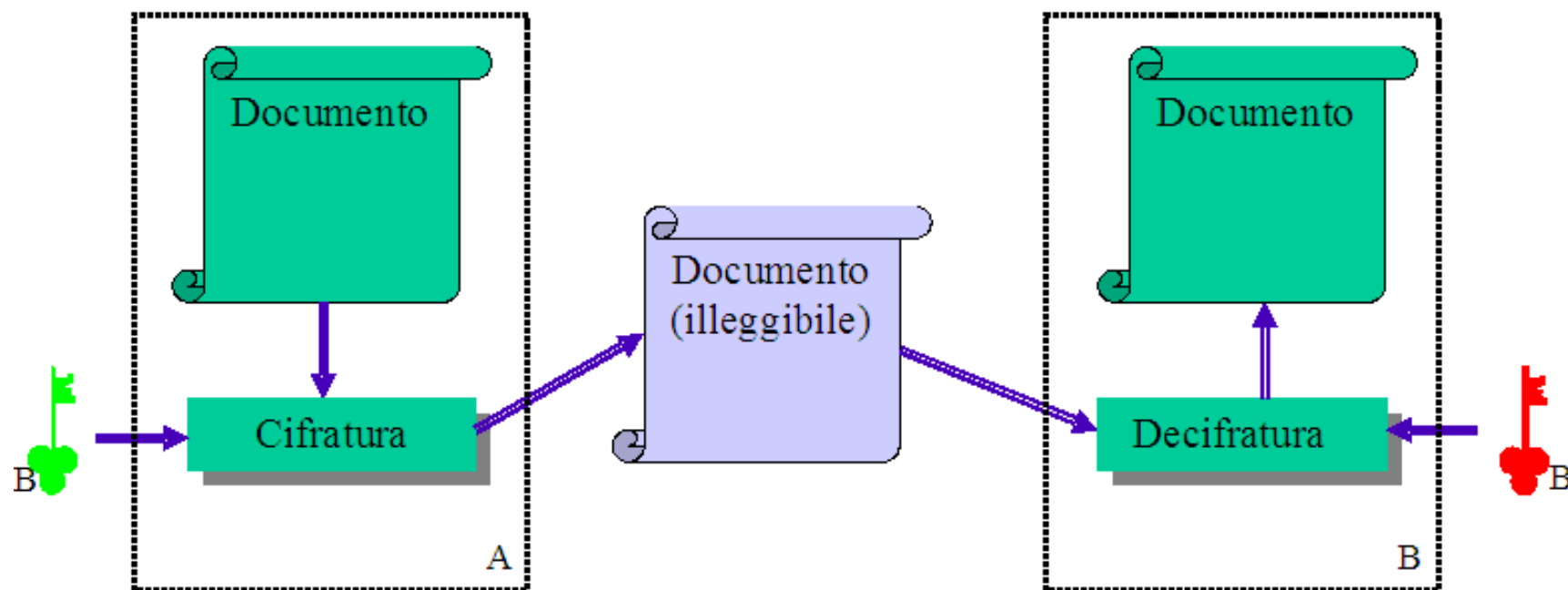
Crittografia Asimmetrica

- Moderna (ufficialmente 1976)
- Basata sulla teoria della complessità computazionale
- Due chiavi correlate ma non (facilmente) calcolabili l'una dall'altra
 - La **chiave privata** è strettamente personale e quindi *identifica* il possessore
 - L'uso di una determinata chiave privata può essere verificato da chiunque per mezzo della corrispondente **chiave pubblica**



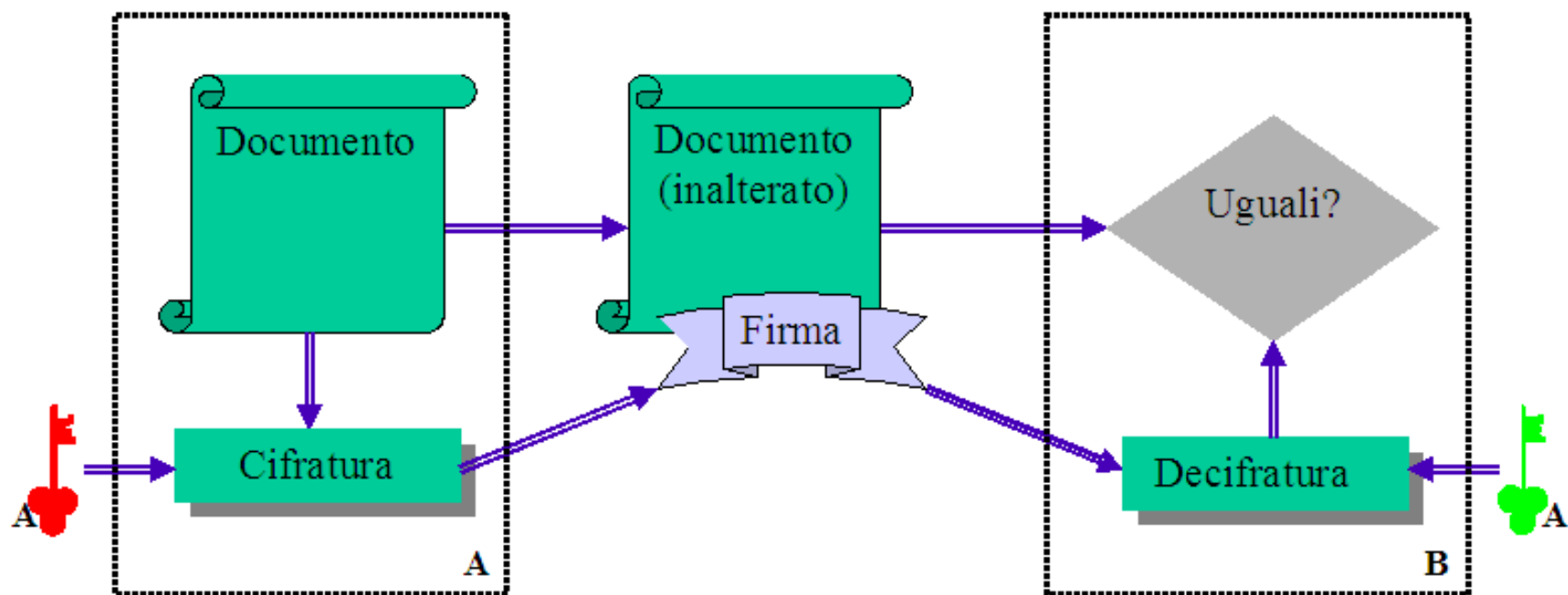
Crittografia Asimmetrica

Procedimento di cifratura



















Firma Digitale

Procedimento di firma



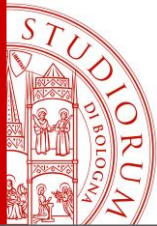
Confronto

	Simmetrica	Asimmetrica
Autenticità		
Integrità		
Riservatezza		
Efficienza		
Robustezza		
Chiavi		
Lunghezza		
Numero per ogni utente		
Protezione		



Biometria

- Componente cardine per la terna di fattori per l'**autenticazione forte**
 - qualcosa che sei, qualcosa che hai, qualcosa che sai
- Problemi non ancora risolti:
 - Ostinatamente usata per l'*identificazione*
 - lunghe operazioni di confronto
 - cattivo bilanciamento tra falsi positivi e falsi negativi
 - Meglio per l'*autenticazione*
 - un solo confronto, minore probabilità di errori
 - Prestazioni più sfumate rispetto ad altre tecniche
 - difficile tuning tra falsi positivi e falsi negativi
 - Impossibilità di sostituzione in caso di compromissione



Sicurezza delle Password

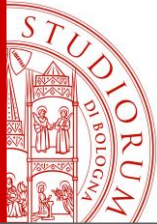
- Aspetto da sempre fondamentale per:
 - impedire l'accesso a utenti non autorizzati
 - nascondere e/o vincolare l'accesso a documenti
- Diverse categorie:
 - Deboli
 - Semplici
 - Intelligenti
 - Strong

Analizzare e Progettare la Sicurezza



Sistema Sicuro, Perché?

- La definizione di una politica di sicurezza deve tenere conto di vincoli tecnici, logistici, amministrativi, politici ed economici, imposti dalla struttura organizzativa in cui il sistema opera
- Per questo serve introdurre la sicurezza sin dalle prime fasi di analisi dei requisiti di un nuovo sistema
 - le vigenti leggi, le politiche e i vincoli aziendali sono la base di partenza per la definizione di un **piano per la sicurezza**



Sistema Sicuro, Perché?

- Un'applicazione o un servizio possono consistere di uno o più componenti funzionali allocati localmente o distribuiti sulla rete
- La sicurezza viene vista come un **processo complesso**, come una catena di caratteristiche
 - dalla computer system security, network security, application-level security sino alle problematiche di protezione dei dati sensibili
- La sfida maggiore lanciata ai progettisti è quella di **progettare applicazioni sicure e di qualità** che tengano conto in modo strutturato di tutti gli aspetti della sicurezza sin dalle prime fasi di analisi del sistema

Sistemi Critici



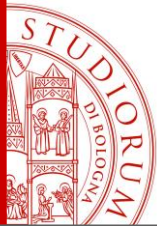
Sistemi Critici

- I **sistemi critici** sono sistemi tecnici o socio-tecnici da cui dipendono persone o aziende
- Se questi sistemi non forniscono i loro servizi come ci si aspetta possono verificarsi seri problemi e importanti perdite
- Ci sono tre tipi principali di sistemi critici:
 - **Sistemi safety-critical**: i fallimenti possono provocare incidenti, perdita di vite umane o seri danni ambientali
 - **Sistemi mission-critical**: i malfunzionamenti possono causare il fallimento di alcune attività e obiettivi diretti
 - **Sistemi business-critical**: i fallimenti possono portare a costi molto alti per le aziende che li usano



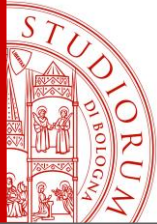
Sistemi Critici

- La proprietà più importante di un sistema critico è la sua **fidatezza**
- Sistema fidato =
disponibilità + affidabilità + sicurezza e protezione
- Ci sono diverse ragioni per le quali la fidatezza è importante:
 - I sistemi non affidabili, non sicuri e non protetti sono rifiutati dagli utenti
 - I costi di un fallimento del sistema potrebbero essere enormi
 - I sistemi inaffidabili possono causare perdita di informazioni



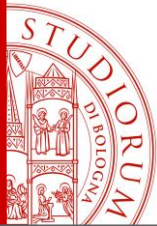
Sistemi Critici

- Componenti del sistema che possono causare fallimenti:
 - Hardware: può fallire a causa di errori nella progettazione, di un guasto a un componente o perché i componenti hanno terminato la loro vita naturale
 - Software: può fallire a causa di errori nelle sue specifiche, nella sua progettazione o nella sua implementazione
 - Operatori umani: possono sbagliare a interagire con il sistema
- Con l'aumentare dell'affidabilità di software e hardware gli errori umani sono diventati la più probabile causa di difetto di un sistema



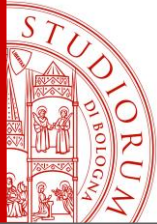
Sistemi Critici

- La sicurezza e la protezione dei sistemi critici sono diventate sempre più importanti con l'aumentare delle connessioni di rete
- Da una parte le connessioni di rete espongono il sistema ad attacchi da parte di malintenzionati
- Dall'altra parte la rete fa in modo che i dettagli delle vulnerabilità siano facilmente divulgati e facilita la distribuzione di patch
- Esempi di attacchi sono:
 - virus
 - usi non autorizzati dei servizi
 - modifiche non autorizzate al sistema e ai suoi dati



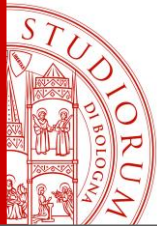
Esempi di Attacchi

- *Exploit*: metodo che sfrutta un bug o una vulnerabilità, per l'acquisizione di privilegi
- *Buffer Overflow*: fornire al programma più dati di quanto esso si aspetti di ricevere, in modo che una parte di questi vadano scritti in zone di memoria dove sono, o dovrebbero essere, altri dati o lo stack del programma stesso
- *Shell code*: sequenza di caratteri che rappresenta un codice binario in grado di lanciare una *shell*, può essere utilizzato per acquisire un accesso alla linea di comando
- *Sniffing*: attività di intercettazione passiva dei dati che transitano in una rete



Esempi di Attacchi

- *Cracking*: modifica di un software per rimuovere la protezione dalla copia, oppure per ottenere accesso a un'area riservata
- *Spoofing*: tecnica con la quale si simula un indirizzo IP privato da una rete pubblica facendo credere agli *host* che l'IP della macchina server da contattare sia il suo
- *Trojan*: programma che contiene funzionalità maliziose; la vittima è indotta a eseguire il programma poiché questo viene spesso inserito nei videogiochi pirati
- *Denial of Service*: il sistema viene forzatamente messo in uno stato in cui i suoi servizi non sono disponibili, influenzando così la disponibilità del sistema



Introduzione alla Security Engineering



Security Engineering

Security Engineering is concerned with how to develop and maintain systems that can resist malicious attacks intended to damage a computer-based system or its data



Da: Software Engineering 8 – I.Sommerville - Addison Wesley – Cap. 30

- L'ingegneria della sicurezza è parte del più vasto campo della sicurezza informatica
- Nell'ingegnerizzazione di un sistema software **non si può** prescindere dalla consapevolezza delle **minacce** che il sistema dovrà affrontare e dei modi in cui tali minacce possono essere neutralizzate

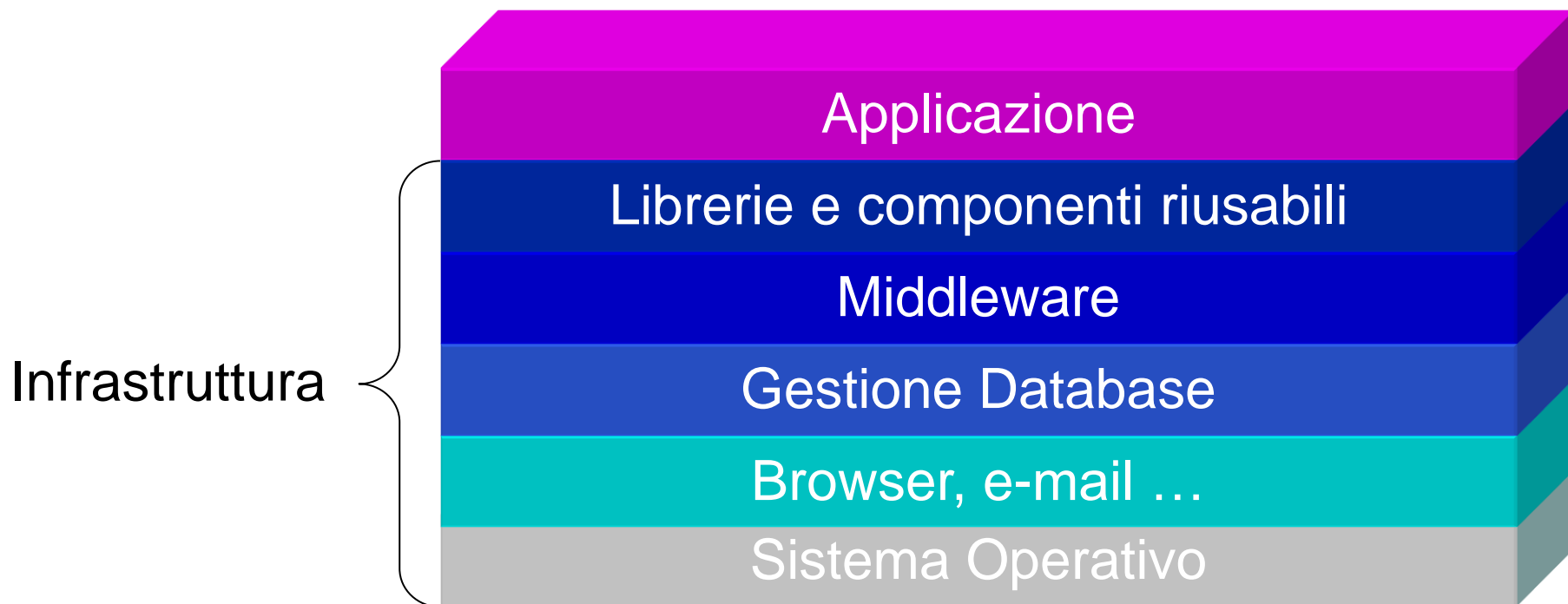


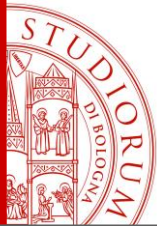
Security Engineering

- Quando si considerano le problematiche di sicurezza nell'ingegnerizzazione di un sistema vanno presi in considerazione due aspetti diversi:
 - la sicurezza dell'applicazione
 - la sicurezza dell'infrastruttura su cui il sistema è costruito



Security Engineering





Applicazione e Infrastruttura

- La sicurezza di una applicazione è un problema di ingegnerizzazione del software dove gli ingegneri devono garantire che il **sistema sia progettato per resistere agli attacchi**
- La sicurezza dell'infrastruttura è invece un problema manageriale nel quale gli amministratori dovrebbero garantire che **l'infrastruttura sia configurata per resistere agli attacchi**
- Gli amministratori dei sistemi devono:
 - inizializzare l'infrastruttura in modo tale che tutti i servizi di sicurezza siano disponibili
 - monitorare e riparare eventuali falle di sicurezza che emergono durante l'uso del software



Gestione della Sicurezza

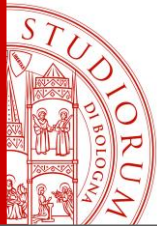
- *Gestione degli utenti e dei permessi:*
 - inserimento e rimozione di utenti dal sistema
 - autenticazione degli utenti
 - creazione di appropriati permessi per gli utenti
- *Deployment e mantenimento del sistema:*
 - installazione e configurazione dei software e del middleware
 - aggiornamento periodico del software con tutte le patch disponibili
- Controllo degli attacchi, rilevazione e ripristino
 - controllo del sistema per accessi non autorizzati
 - identificazione e messa in opera di strategie contro gli attacchi
 - backup per ripristinare il normale utilizzo dopo un attacco

Glossario e Minacce



Sicurezza: Glossario

- **Bene** (Asset): una risorsa del sistema che deve essere protetta
- **Esposizione** (Exposure): possibile perdita o danneggiamento come risultato di un attacco andato a buon fine
 - Potrebbe essere una perdita o un danneggiamento di dati o una perdita di tempo nel ripristino del sistema dopo l'attacco
- **Vulnerabilità** (Vulnerability): una debolezza nel sistema software che potrebbe essere sfruttata per causare una perdita o un danno
- **Attacco** (Attack): sfruttamento di una vulnerabilità del sistema
- **Minaccia** (Threat): circostanza che ha le potenzialità per causare perdite e danni
- **Controllo** (Control): una misura protettiva che riduce una vulnerabilità del sistema



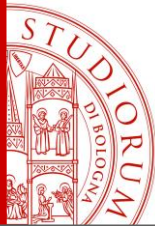
Tipi di Minacce

- *Minacce alla riservatezza del sistema o dei suoi dati:*
le informazioni possono essere svelate a persone o programmi non autorizzati
- *Minacce all'integrità del sistema o dei suoi dati:*
i dati o il software possono essere danneggiati o corrotti
- *Minacce alla disponibilità del sistema o dei suoi dati:*
può essere negato l'accesso agli utenti autorizzati al software o ai dati
- Queste minacce sono interdipendenti
 - Se un attacco rende il sistema non disponibile, la modifica sulle informazioni potrebbe non avvenire, rendendo così il sistema non integro



Tipi di Controllo

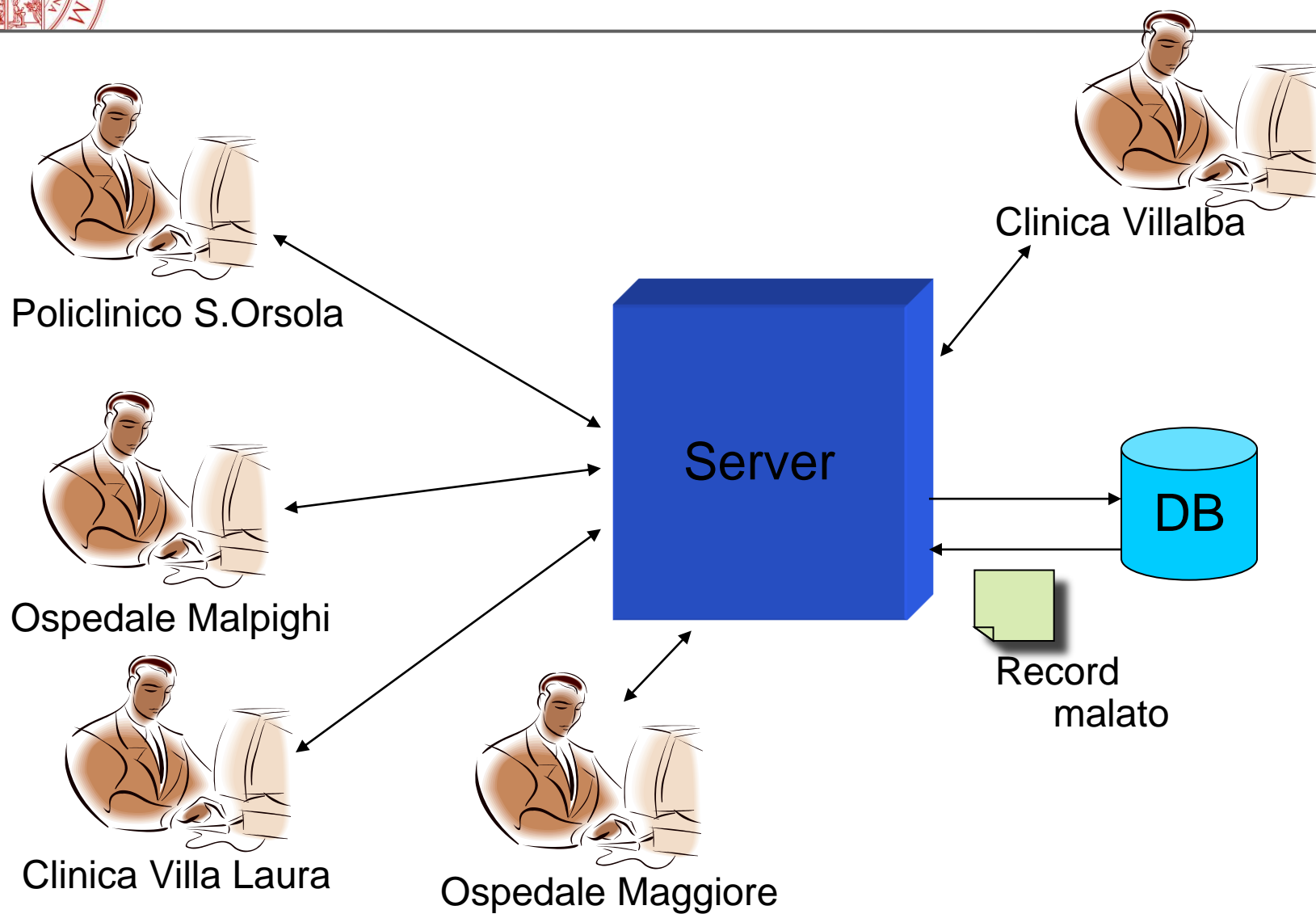
- *Controlli per garantire che gli attacchi non abbiano successo:*
la strategia è quella di progettare il sistema in modo da evitare i problemi di sicurezza
 - i sistemi militari sensibili non sono connessi alla rete pubblica
 - crittografia
- *Controlli per identificare e respingere attacchi:*
la strategia è quella di monitorare le operazioni del sistema e identificare pattern di attività atipici, nel caso agire di conseguenza (spegnere parti del sistema, restringere l'accesso agli utenti, ..)
- *Controlli per il ripristino*
 - backup, replicazione, polizze assicurative

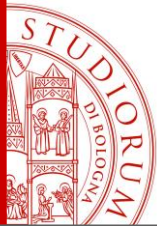


Esempio

- Un sistema informativo ospedaliero mantiene le informazioni personali sui pazienti e sui loro trattamenti
- Il sistema deve essere accessibile da differenti ospedali e cliniche attraverso un'interfaccia web
- Lo staff ospedaliero deve utilizzare una specifica coppia <username, password> per autenticarsi, dove lo username è il nome del dipendente
- Il sistema richiede password che siano lunghe almeno 8 caratteri, ma consente ogni password senza ulteriori verifiche

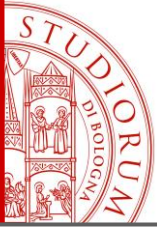
Schema Logico



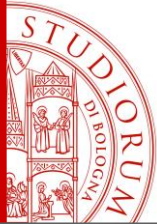


Esempio

Termine	Descrizione
Beni	I record dei pazienti che ricevono o hanno ricevuto trattamenti sanitari; il database; il sistema informativo
Esposizione	Possibile perdita di futuri pazienti che non si fidano della clinica. Perdita finanziaria e perdita d'immagine
Vulnerabilità	Un sistema di password debole rende facile agli utenti la memorizzazione di password banali; lo username è uguale al nome del dipendente
Attacchi	Furto di identità di un utente autorizzato e successiva violazione e sottrazione di dati; denial of service
Minacce	Possibilità di indovinare le password di utenti autorizzati; arrivo contemporaneo di un numero elevato di richieste
Controllo	Sistema di controllo delle password che obblighi gli utenti a utilizzare password di tipo strong; replicazione del servizio su più server



Analisi del Rischio



Analisi del Rischio

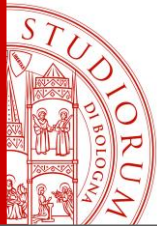
- L'analisi del rischio si occupa di
 - valutare le possibili perdite che un attacco può causare ai beni di un sistema
 - bilanciare queste perdite con i costi richiesti per la protezione dei beni stessi

costo protezione << costo della perdita



Analisi del Rischio

- L'analisi del rischio è una problematica più manageriale che tecnica
- Il ruolo degli ingegneri della sicurezza è quindi quello di fornire una **guida tecnica e giuridica** sui problemi di sicurezza del sistema
- Sarà poi compito dei manager decidere se accettare i costi della sicurezza o i rischi che derivano dalla mancanza di procedure di sicurezza
- L'analisi del rischio inizia dalla valutazione delle politiche di sicurezza organizzazionali che spiegano cosa dovrebbe e cosa non dovrebbe essere consentito fare

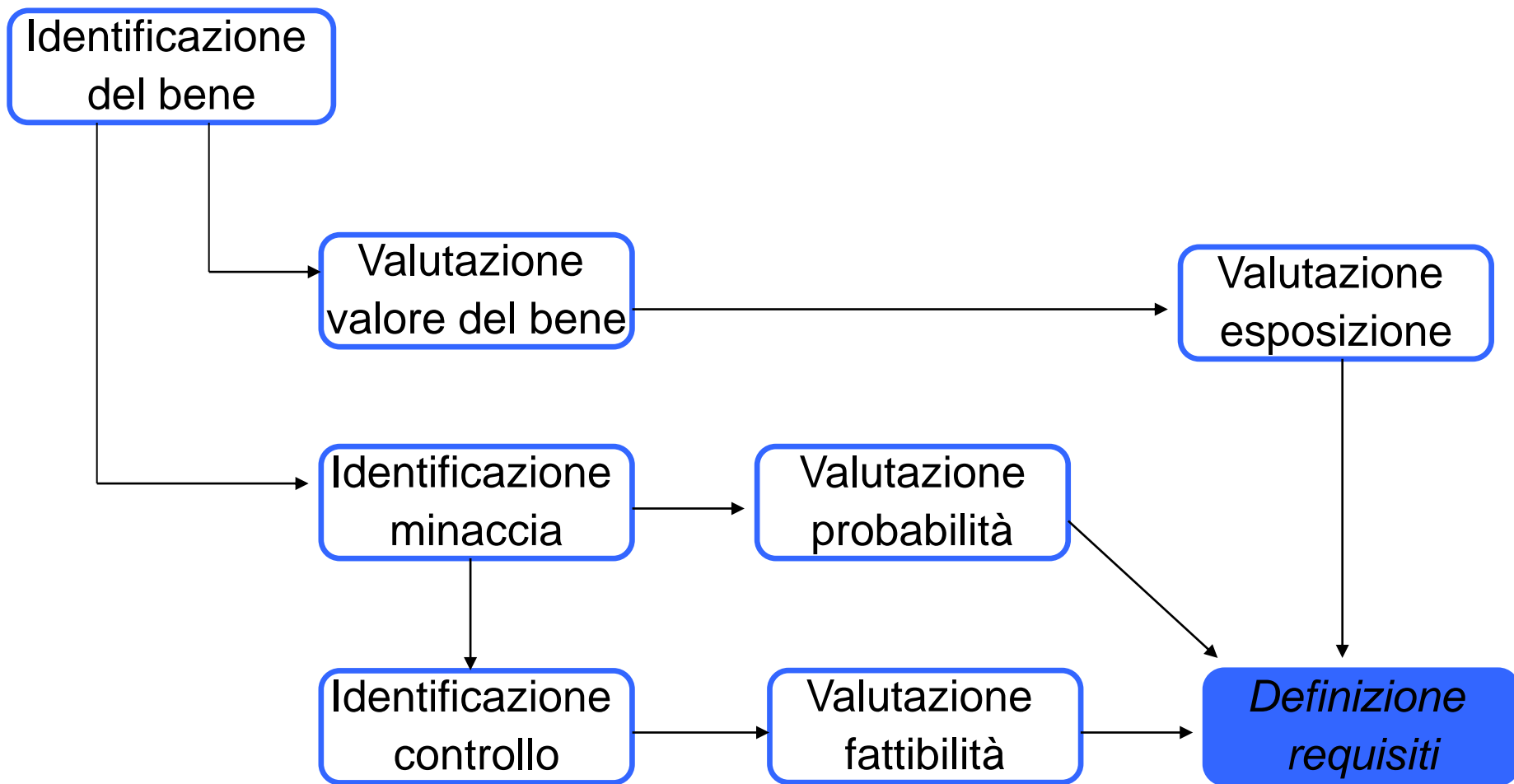


Analisi del Rischio

- Le politiche di sicurezza propongono le condizioni che dovrebbero sempre essere mantenute dal sistema di sicurezza, quindi aiutano ad identificare le minacce che potrebbero sorgere
- La valutazione del rischio è un processo in più fasi:
 - **valutazione preliminare del rischio:**
determina i requisiti di sicurezza dell'intero sistema
 - **ciclo di vita della valutazione del rischio:**
avviene contestualmente e segue il ciclo di vita dello sviluppo del software



Valutazione Preliminare del Rischio

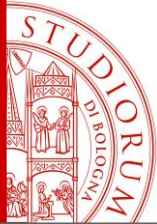


Identificazione del bene



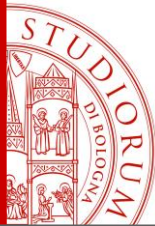
Analisi del Sistema Informatico

- Durante questa fase si può stabilire la seguente agenda delle attività:
 - Analisi delle risorse fisiche
 - Analisi delle risorse logiche
 - Analisi delle dipendenze fra risorse



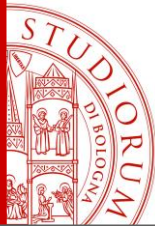
Analisi delle Risorse Fisiche

- In questa attività, il sistema informatico viene visto come insiemi di dispositivi che, per funzionare, hanno bisogno di spazio, alimentazione, condizioni ambientali adeguate, protezioni da furti e danni materiali
- In particolare occorre:
 - individuare sistematicamente tutte le risorse fisiche
 - ispezionare e valutare tutti i locali che ospiteranno le risorse fisiche
 - verificare la cablatura dei locali



Analisi delle Risorse Logiche

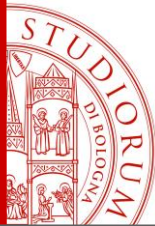
- Il sistema viene visto come insieme di informazioni, flussi e processi
- In particolare occorre:
 - **Classificare le informazioni** in base al valore che hanno per l'organizzazione, il grado di riservatezza e il contesto di appartenenza
 - **Classificare i servizi** offerti dal sistema informatico affinché non presentino effetti collaterali pericolosi per la sicurezza del sistema



Analisi delle Dipendenze tra Risorse

- Per ciascuna risorsa (fisica o logica) occorre individuare di quali altre risorse essa ha bisogno per funzionare correttamente
- Questa analisi tende ad evidenziare le risorse **potenzialmente critiche**, ovvero quelle da cui dipende il funzionamento di un elevato numero di altre risorse
- I risultati di questa analisi sono usati anche nella fase di valutazione del rischio
 - in particolare, sono di supporto allo studio della propagazione dei malfunzionamenti a seguito dell'occorrenza di eventi indesiderati

Identificazione delle minacce



Identificazione delle Minacce

- In questa fase si cerca di definire quello che non deve poter accadere nel sistema
- Si parte dal considerare come evento indesiderato ***qualsiasi accesso che non sia esplicitamente permesso***
- A tal fine è possibile in generale distinguere tra
 - attacchi intenzionali
 - eventi accidentali



Attacchi Intenzionali

- Gli attacchi vengono caratterizzati in funzione della risorsa (sia fisica che logica) che viene attaccata e delle possibili tecniche usate per l'attacco
- Le tecniche di attacco possono essere classificate in funzione del livello al quale operano
- Si distingue tra **tecniche a livello fisico** e **a livello logico**
- Gli attacchi a livello fisico sono principalmente tesi **a sottrarre o danneggiare le risorse critiche**
- Si tratta di
 - *Furto* = un attacco alla disponibilità e alla riservatezza
 - *Danneggiamento* = un attacco alla disponibilità e alla integrità



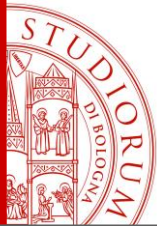
Attacchi a Livello Logico

- Gli attacchi a livello logico sono principalmente tesi a **sottrarre informazione** o degradare l'operatività del sistema
- Dal punto di vista dei risultati che è indirizzato a conseguire un attacco logico può essere classificato come:
 - **Intercettazione e deduzione** (attacco alla riservatezza): sniffing, spoofing, emulatori...
 - **Intrusione** (attacco all'integrità e alla riservatezza): IP-spoofing, backdoor...
 - **Disturbo** (attacco alla disponibilità): virus, worm, denial of service...



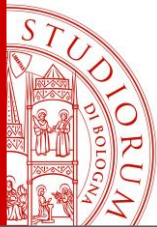
Eventi Accidentali

- Una possibile casistica degli eventi accidentali che accadono più di frequente:
 - **a livello fisico:**
 - guasti ai dispositivi che compongono il sistema
 - guasti di dispositivi di supporto (es. condizionatori)
 - **a livello logico:**
 - perdita di password o chiave hardware
 - cancellazione di file
 - corruzione del software di sistema
(ad esempio, a seguito dell'installazione di estensioni incompatibili)



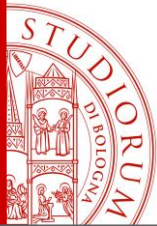
Valutazione dell'Esposizione

- A ogni minaccia occorre associare un *rischio* così da indirizzare l'attività di individuazione delle contromisure verso le aree più critiche
- Per *rischio* s'intende una combinazione della probabilità che un evento accada con il danno che l'evento può arrecare al sistema
- Nel valutare il danno si tiene conto
 - delle *dipendenze tra le risorse*
 - dell'eventuale propagazione del malfunzionamento



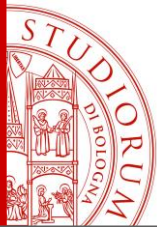
Valutazione delle Probabilità: Attacchi Intenzionali

- La probabilità di occorrenza di **attacchi intenzionali** dipende principalmente dalla **facilità** di attuazione e dai **vantaggi** che potrebbe trarne l'intruso
 - Il danno si misura come **grado di perdita** dei tre requisiti fondamentali (riservatezza, integrità, disponibilità)
- MA l'attaccante **applicherà sempre tutte le tecniche** di cui dispone, su tutte le risorse attaccabili
→ necessità di valutare anche il rischio di un **attacco composto**
 - **un insieme di attacchi** elementari concepiti con un medesimo obiettivo e **condotti in sequenza**



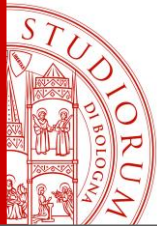
Individuazione del Controllo

- Occorre scegliere il controllo da adottare per neutralizzare gli attacchi individuati:
 - Valutazione del rapporto costo/efficacia
 - Analisi di standard e modelli di riferimento
 - Controllo di carattere organizzativo
 - Controllo di carattere tecnico



Valutazione del Rapporto Costo/Efficacia

- Valuta **il grado di adeguatezza** di un controllo
- Mira ad evitare che i controlli presentino un **costo ingiustificato** rispetto al rischio dal quale proteggono
- **Efficacia del controllo** definita come *funzione del rischio* rispetto agli eventi indesiderati che neutralizza
- Il costo di un controllo deve essere calcolato senza dimenticare i **costi nascosti**



Costi Nascosti

- Occorre tenere presenti le **limitazioni** che i controlli impongono e le **operazioni di controllo** che introducono nel flusso di lavoro del sistema informatico e dell'organizzazione
- Le principali voci di costo sono le seguenti:
 - costo di messa in opera del controllo
 - peggioramento dell'ergonomia dell'interfaccia utente
 - decadimento delle prestazioni del sistema nell'erogazione dei servizi
 - aumento della burocrazia



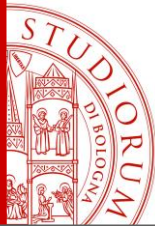
Controlli di Carattere Organizzativo

- **Condizione essenziale** affinché la tecnologia a protezione del sistema informatico risulti efficace è che venga **utilizzata nel modo corretto** da personale pienamente **consapevole**
- Devono quindi essere definiti con precisione **ruoli** e **responsabilità** nella gestione sicura di tale sistema
- Per ciascun ruolo, dall'amministratore al semplice utente, devono essere definite **norme comportamentali** e **procedure precise** da rispettare



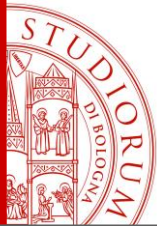
Controlli di Carattere Tecnico

- Controlli di base
 - a livello del sistema operativo e dei servizi di rete
- Controlli specifici del particolare sistema
 - si attestano normalmente a livello applicativo
- Controlli tecnici più frequenti
 - configurazione sicura del sistema operativo di server e postazioni di lavoro (contromisura di base)
 - confinamento logico delle applicazioni server su server dedicati



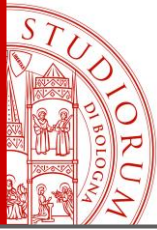
Controlli di Carattere Tecnico

- Etichettatura delle informazioni, allo scopo di avere un controllo più fine dei diritti di accesso
- Moduli software di cifratura integrati con le applicazioni
- Apparecchiature di telecomunicazione in grado di cifrare il traffico dati in modo trasparente alle applicazioni
- Firewall e server proxy in corrispondenza di eventuali collegamenti con reti TCP/IP
- Chiavi hardware e/o dispositivi di riconoscimento degli utenti basati su rilevamenti biofisici



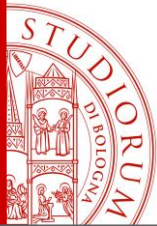
Integrazione dei Controlli

- Un insieme di controlli non deve presentarsi come una **“collezione di espedienti”** non correlati tra loro
- È importante integrare i vari controlli in una **politica di sicurezza** organica
- **Operare una selezione** dei controlli adottando un **sottoinsieme di costo minimo** che rispetti alcuni **vincoli**:
 - **completezza delle contromisure**
 - **omogeneità delle contromisure**
 - **ridondanza controllata delle contromisure**
 - **effettiva attuabilità delle contromisure**



Vincoli del Sottoinsieme

- Completezza:
il sottoinsieme deve fare fronte a tutti gli eventi indesiderati
- Omogeneità:
le contromisure devono essere compatibili e integrabili tra loro
- Ridondanza controllata:
la ridondanza delle contromisure ha un costo e deve essere rilevata e vagliata accuratamente
- Effettiva attuabilità:
l'insieme delle contromisure deve rispettare tutti i vincoli imposti dall'organizzazione nella quale andrà ad operare



Esempio

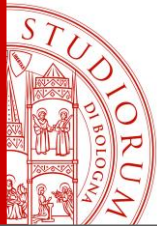
- Torniamo all'esempio del sistema per la gestione di dati ospedalieri
- Quali sono i beni del sistema?
 - il sistema informativo
 - il database dei pazienti
 - i record di ogni paziente
- Quali sono le minacce?
 - furto identità dell'amministratore
 - furto identità di utente autorizzato
 - DoS



Esempio

Valutazione del Bene

Bene	Valore	Esposizione
Sistema Informativo	Alto. Supporto a tutte le consultazioni cliniche	Alta. Perdita finanziaria; costi ripristino sistema; danni a pazienti se cure non date
Database pazienti	Alto. Supporto a tutte le consultazioni cliniche Critico dal punto di vista della sicurezza	Alta. Perdita finanziaria; costi ripristino sistema; danni a pazienti se cure non date
Record paziente	Normalmente basso. Potrebbe essere alto per pazienti particolari	Perdita diretta bassa, ma possibile perdita di reputazione della clinica



Esempio

Analisi Minacce e Controlli

Minaccia	Probabilità	Controllo	Fattibilità
Furto identità Amministratore	Bassa	Accesso solo da postazioni specifiche fisicamente sicure	Basso costo implementativo ma attenzione alla distribuzione delle chiavi
Furto identità utente	Alta	Meccanismi biometrici	Molto costoso e non accettato
		Log di tutte le operazioni	Semplice, trasparente e supporta il ripristino
DoS	Media	Progettazione adeguata, controllo e limitazione degli accessi	Basso costo. Impossibile prevedere e impedire questo tipo di attacco



Esempio

Requisiti di Sicurezza

- Alcuni dei requisiti ricavati dalla valutazione preliminare dei rischi
 - le informazioni relative ai pazienti devono essere scaricate all'inizio della sessione clinica dal database e memorizzate in un'area sicura sul client
 - le informazioni relative ai pazienti non devono essere mantenute sul client dopo la chiusura della sessione clinica
 - deve essere mantenuto un log su una macchina diversa dal server che memorizzi tutti i cambiamenti effettuati sul database



Villaggio Turistico

Valutazione del Bene

Bene	Valore	Esposizione
Sistema Informativo	Alto. Supporto a tutta la gestione del villaggio turistico	Alta. Perdita finanziaria e di immagine
Informazioni relative agli Ospiti	Medio. Dati generali degli ospiti del villaggio turistico	Media. Perdita di immagine se vengono divulgati dati degli Ospiti
Informazioni relative alle GuestCard	Alto. L'elenco degli acquisti è associato alle GuestCard	Molto Alta. Perdita finanziaria nel caso gli Ospiti contestino acquisti ingiustamente addebitati. Perdita di immagine
Informazioni relative alle vendite	Alto. Sulla base dei movimenti nei PuntidiVendita, la CatenaPuntiVendita gestisce i magazzini e i dati fiscali	Alta. Perdita finanziaria se i dati delle vendite e delle forniture non coincidono. Perdita di immagine se il servizio che vuole essere acquistato per qualche motivo non è presente
Informazioni relative al personale	Alto. Ci sono tutte le informazioni relative al personale, comprese le credenziali di accesso	Alta. Perdita finanziaria, se vengono rubate le credenziali del personale si possono perpetuare svariate frodi. Perdita di immagine



Villaggio Turistico

Analisi Minacce e Controlli

Minaccia	Probabilità	Controllo	Fattibilità
Furto credenziali Operatore	Alta. La username è fissata e facile da identificare	Accesso da macchine sicure	Basso costo di realizzazione ma attenzione se le macchine vengono lasciate incustodite
		Log delle Operazioni	Basso costo implementativo
Furto credenziali personale dei punti di vendita	Alta. La username è fissata e facile da identificare	Accesso da macchine sicure	Basso costo di realizzazione ma attenzione se le macchine vengono lasciate incustodite
		Log delle Operazioni	Basso costo implementativo
Intercettazione comunicazioni	Alta. Il sistema è distribuito e client/server avvengono tantissime interazioni tra i diversi client e il server.	Cifratura delle comunicazioni	Il costo dipende dal tipo di cifratura scelto. Se simmetrica basso, se asimmetrica più alto dovuto alla necessità di rilascio di coppie di chiavi da un ente di certificazione
		Log di tutte le operazioni	Basso costo implementativo
DoS	Bassa	Progettazione adeguata, controllo e limitazione degli accessi	Basso costo. Impossibile prevenire un DoS

Ciclo di vita della valutazione del rischio



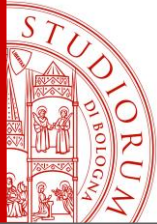
Ciclo di Vita della Valutazione del Rischio

- È necessaria la conoscenza dell'architettura del sistema e dell'organizzazione dei dati
- La piattaforma e il middleware sono già stati scelti, così come la strategia di sviluppo del sistema
- Questo significa che si hanno molti più dettagli riguardo a che cosa è necessario proteggere e sulle possibili vulnerabilità del sistema
- Le vulnerabilità possono essere “ereditate” dalle scelte di progettazione ma non solo
- La valutazione del rischio dovrebbe essere parte di tutto il ciclo di vita del software: dall'ingegnerizzazione dei requisiti al deployment del sistema



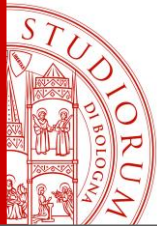
Ciclo di Vita della Valutazione del Rischio

- Il processo seguito è simile a quello della valutazione preliminare dei rischi, con l'aggiunta di attività riguardanti l'identificazione e la valutazione delle vulnerabilità
- La valutazione delle vulnerabilità identifica i beni che hanno più probabilità di essere colpiti da tali vulnerabilità
- Vengono messe in relazione le vulnerabilità con i possibili attacchi al sistema
- Il risultato della valutazione del rischio è un insieme di decisioni ingegneristiche che influenzano la progettazione o l'implementazione del sistema o limitano il modo in cui esso è usato

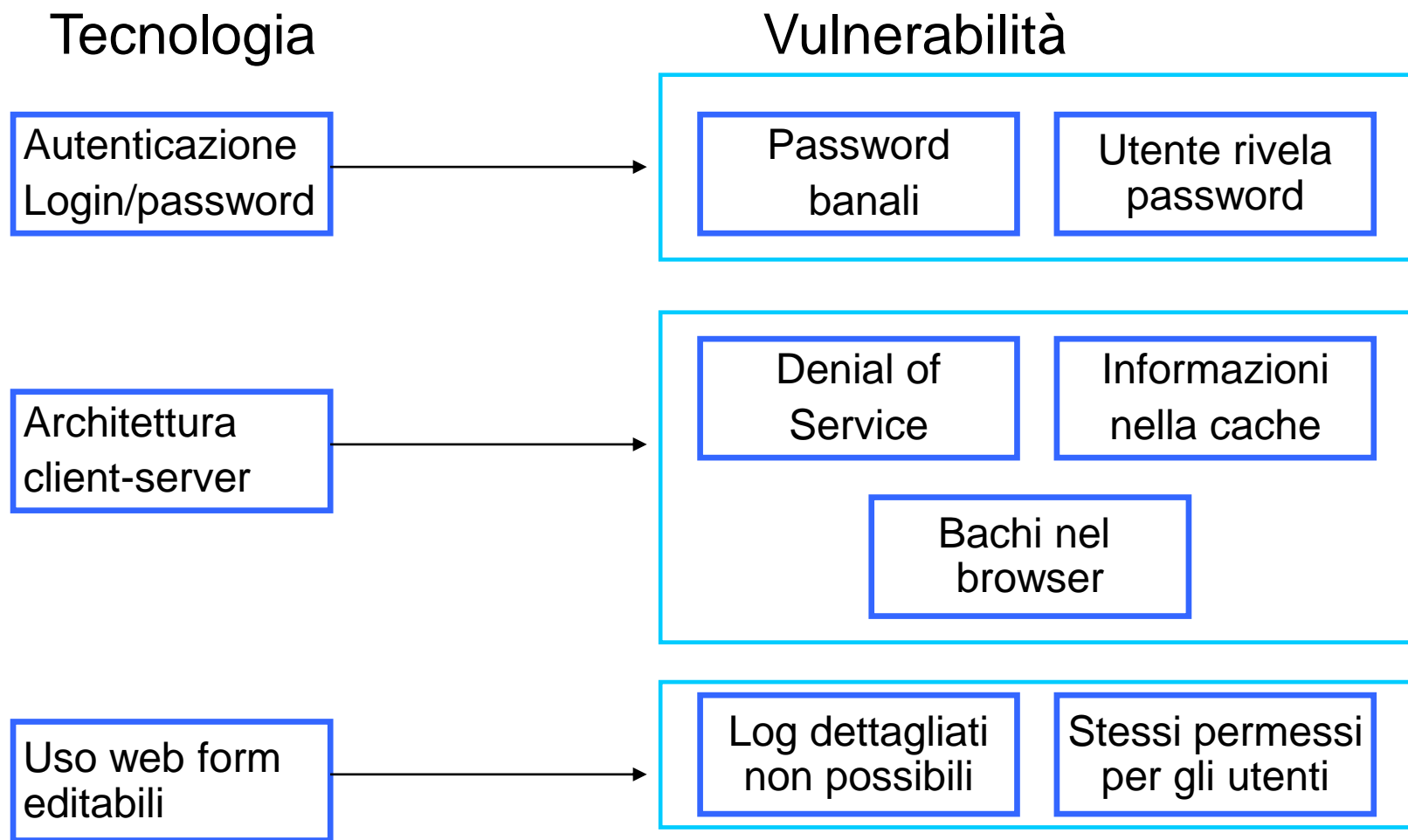


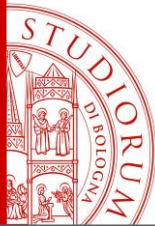
Esempio

- Si supponga che il provider dei servizi ospedalieri decida di acquistare un prodotto commerciale per la gestione dei dati dei pazienti
- Questo sistema deve essere configurato per ogni tipo di clinica in cui è utilizzato
- Scelte progettuali del sistema acquistato:
 - autenticazione solo con username e password
 - architettura client-server: il client accede attraverso un'interfaccia web standard
 - l'informazione è presentata agli utenti attraverso una web form editabile, è quindi possibile modificare le informazioni



Esempio: Vulnerabilità





Esempio

- Valutate le vulnerabilità del sistema adottato
si deve decidere quali mosse attuare
al fine di limitare i rischi associati
- Introduzione di **nuovi requisiti di sicurezza**
- Introduzione di un meccanismo di verifica delle password
 - l'accesso al sistema deve essere permesso
solo ai client approvati e registrati dall'amministratore
 - tutti i client devono avere un solo browser installato
e approvato dall'amministratore



Villaggio Turistico

Vulnerabilità

Tecnologia	Vulnerabilità
Autenticazione username/password	<ul style="list-style-type: none">• Password banali• Utente rivela volontariamente password• Utente rivela password a seguito di un attacco di Ingegneria Sociale
Cifratura comunicazioni	<p>Le vulnerabilità dipendono dal tipo di cifratura.</p> <p>Cifratura Simmetrica:</p> <ul style="list-style-type: none">• Tempo di vita della chiave. Più informazioni cifro con la stessa chiave più materiale offro per l'analisi del testo ad un attaccante• Lunghezza della chiave• Memorizzazione della chiave <p>Cifratura Asimmetrica:</p> <ul style="list-style-type: none">• Memorizzazione chiave privata
Architettura Client/Server	<ul style="list-style-type: none">• DoS• Man in the Middle• Sniffing delle comunicazioni

Security Use Case e Misuse Case

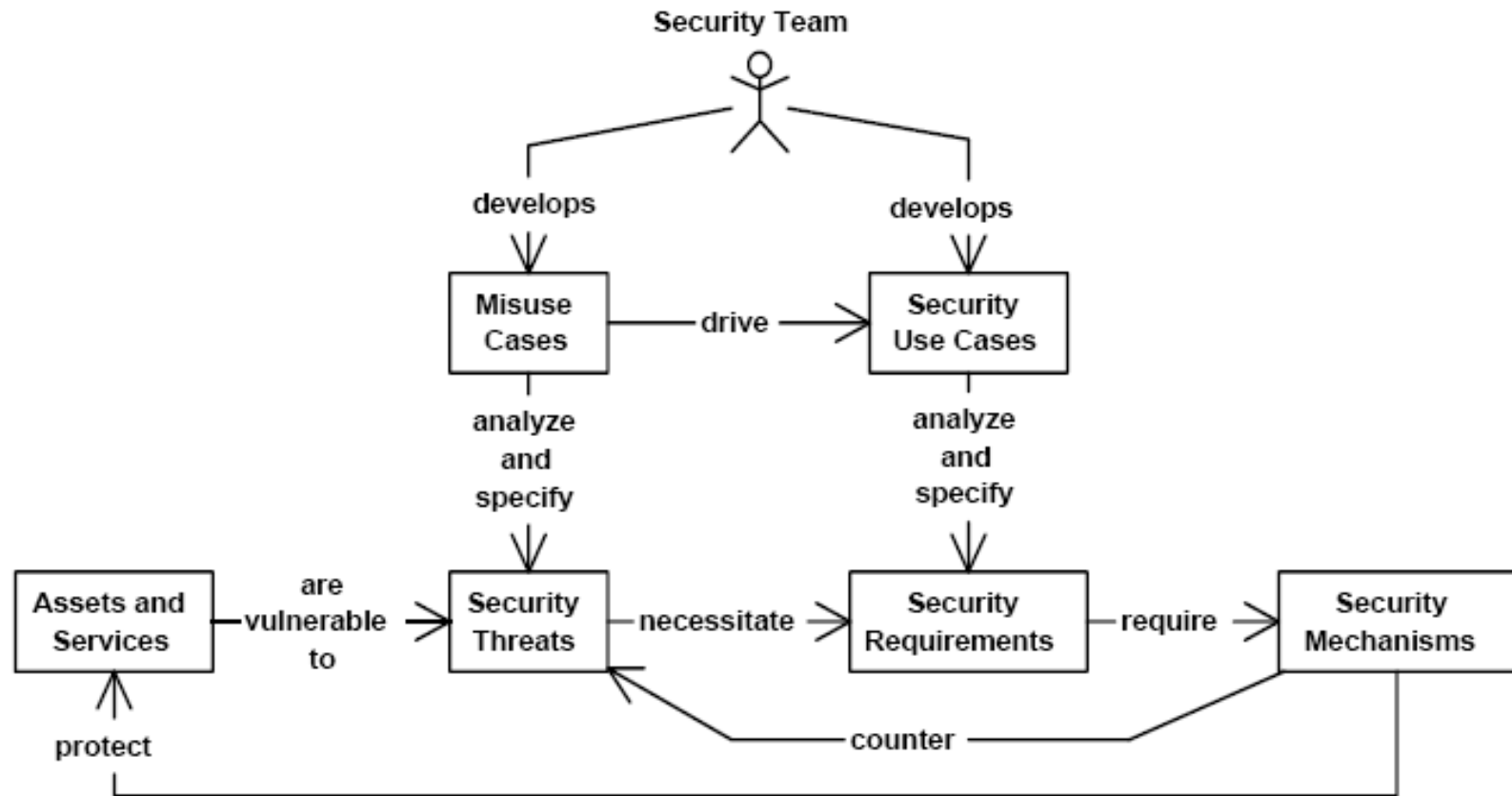


Security Use Case e Misuse Case

- I **misuse case** si concentrano sulle interazioni tra l'applicazione e gli attaccanti che cercano di violarla
- La condizione di successo di un misuse case è l'attacco andato a buon fine
- Questo li rende particolarmente adatti per analizzare le minacce, ma non molto utili per la determinazione dei requisiti di sicurezza
- È invece compito dei **security use case** specificare i requisiti tramite i quali l'applicazione dovrebbe essere in grado di proteggersi dalle minacce



Security Use Case e Misuse Case



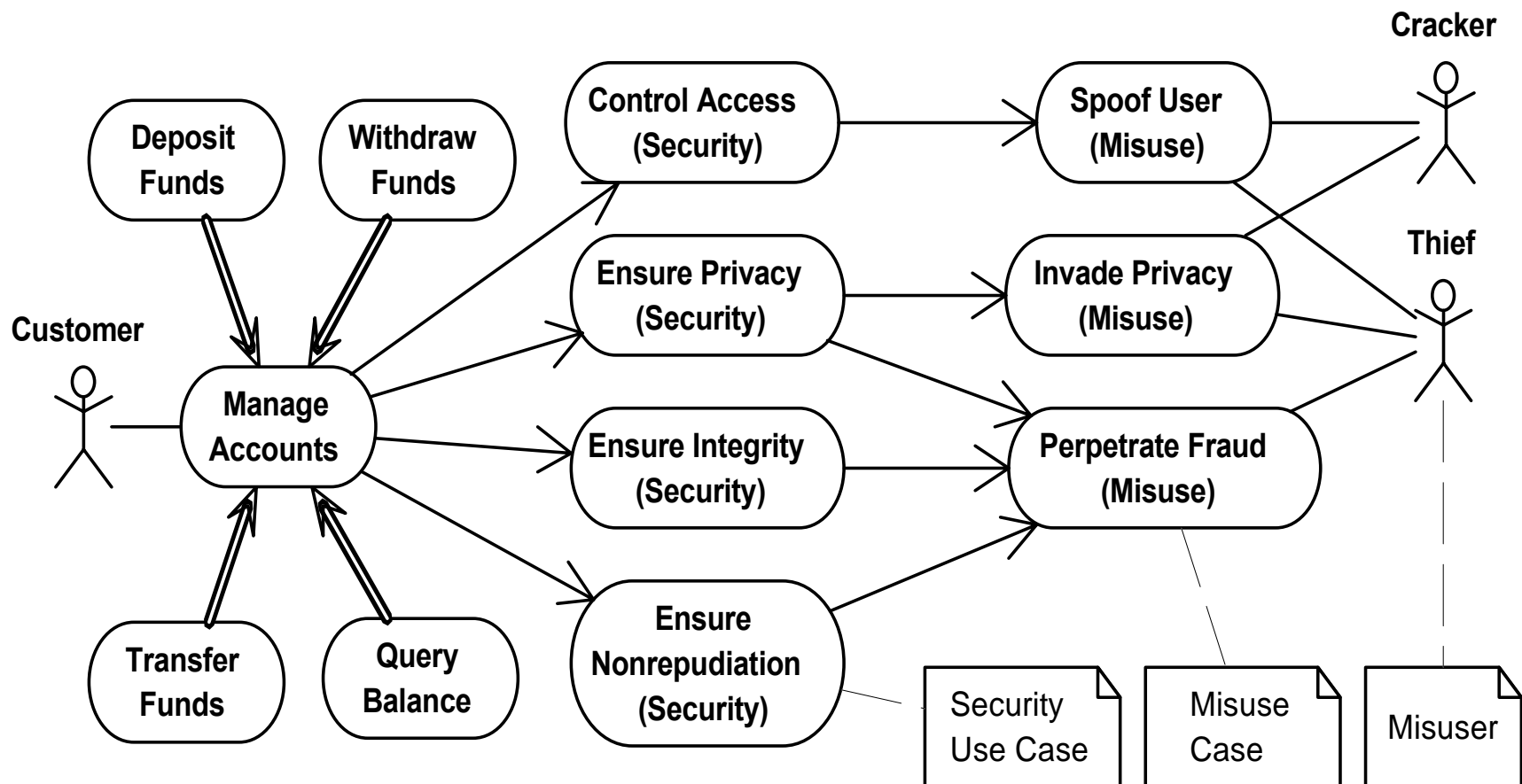
Security Use Cases - Donald G. Firesmith- JOT Vol. 2, No. 3, May-June 2003



Security Use Case e Misuse Case

	Misuse Case	Security Use Case
Uso	Analizzare e specificare le minacce	Analizzare e specificare i requisiti di sicurezza
Criteri di successo	Successo attaccanti	Successo applicazione
Prodotto da	Security Team	Security Team
Usato da	Security Team	Requirements Team
Attori Esterni	Attaccanti, Utenti	Utenti
Guidato da	Analisi vulnerabilità dei beni e analisi minacce	Misuse case

Esempio



Security Use Cases - Donald G. Firesmith- JOT Vol. 2, No. 3, May-June 2003

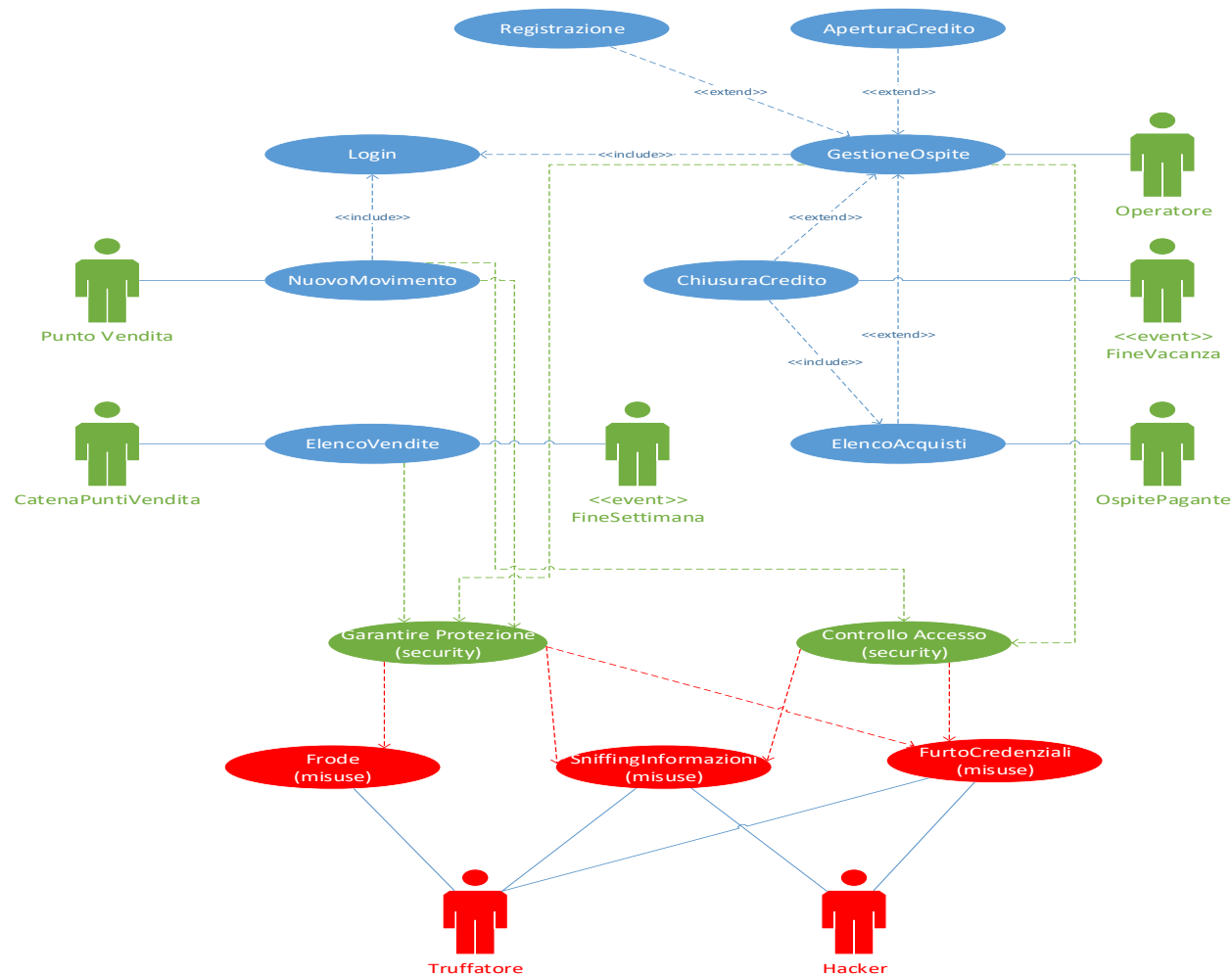
Esempio: Scenario

Use Case: Integrity			
Use Case Path: System Message Integrity			
Security Threat: A misuser corrupts a message that is sent from the system to a user.			
Preconditions: 1) The misuser has the means to intercept a message from the system to a user. 2) The misuser has the means to modify an intercepted message. 3) The misuser has the means to forward the modified message to the user.			
User Interactions	Misuser Interactions	System Requirements	
		System Interactions	System Actions
		The system shall send a message to a user.	The system shall ensure that modifications to the message will be obvious to the user.
	The misuser intercepts and modifies the system's message and forwards it on to the user.		
The user receives the corrupted message.			The system shall recognize that its message was corrupted.
		The system shall notify the user that its message was corrupted.	
Postconditions: The system shall have notified the user that the system's message was corrupted.			

Security Use Cases - Donald G. Firesmith- JOT Vol. 2, No. 3, May-June 2003

Villaggio Turistico

Gestione Villaggio Turistico





Villaggio Turistico

Titolo	ControlloAccesso	
Descrizione	Gli accessi al sistema devono essere controllati	
Misuse case	SniffingInformazioni, FurtoCredenziali	
Relazioni		
Precondizioni	L'Attaccante ha i mezzi per scoprire almeno la username di Operatori e personale dei punti vendita	
Postcondizioni	Il Sistema blocca momentaneamente l'accesso all'utente e notifica un tentativo di accesso fraudolento	
Scenario principale	Sistema	Attaccante
		Dopo aver scoperto qualche username tenta di accedere al sistema inserendo password con un attacco con dizionario
	Controlla le credenziali immesse e blocca l'accesso nel caso tali credenziali risultino errate dopo un certo numero di tentativi.	
Scenario di attacco avvenuto con successo	Sistema	Attaccante
		Attacco con dizionario riuscito
	Il Sistema controlla le credenziali immesse e consente l'accesso al sistema	
		Naviga tra le maschere del sistema e cerca di carpire più informazioni possibili
	Il Sistema scrive nel log tutte le operazioni eseguite dall'utente	
	Il Sistema controlla periodicamente il log alla ricerca di pattern di accesso atipici e se rilevati notifica un accesso fraudolento	



Security Use Case: Linee Guida

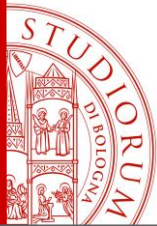
- I casi d'uso non ***dovrebbero mai specificare meccanismi*** di sicurezza
 - Le decisioni relative ai meccanismi devono essere lasciate alla progettazione
- Requisiti attentamente differenziati dalle informazioni secondarie
 - interazioni del sistema, azioni del sistema e post-condizioni sono i soli requisiti
- ***Evitare di specificare vincoli progettuali non necessari***
- Documentare esplicitamente i percorsi individuali attraverso i casi d'uso al fine di specificare i reali requisiti di sicurezza
- Basare i security use case su differenti tipi di requisiti di sicurezza fornisce una naturale organizzazione dei casi d'uso



Security Use Case: Linee Guida

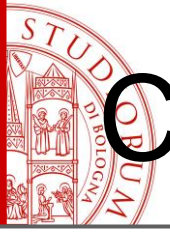
- Documentare le minacce alla sicurezza che giustificano i percorsi individuali attraverso i casi d'uso
- Distinguere chiaramente tra interazioni degli utenti e degli attaccanti
- Distinguere chiaramente tra le interazioni che sono visibili esternamente e le azioni nascoste del sistema
- Documentare sia le precondizioni che le post-condizioni che catturano l'essenza dei percorsi individuali

SPECIFICA DEI REQUISITI DI SICUREZZA



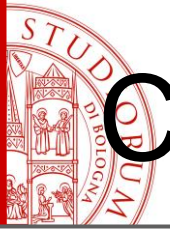
Requisiti di Sicurezza

- Non è sempre possibile specificare i requisiti associati alla sicurezza in **modo quantitativo**
- Quasi sempre questa tipologia dei requisiti è espressa nella forma “**non deve**”
 - definisce comportamenti inaccettabili per il sistema
 - non definisce funzionalità richieste al sistema
- L’approccio convenzionale della specifica dei requisiti è basato sul contesto, sui beni da proteggere e sul loro valore per l’organizzazione



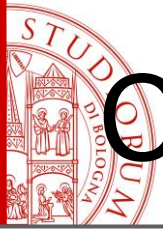
Categorie Requisiti di Sicurezza

- *Requisiti di identificazione*
 - specificano se un sistema deve identificare gli utenti prima di interagire con loro
- *Requisiti di autenticazione*
 - specificano come identificare gli utenti
- *Requisiti di autorizzazione*
 - specificano i privilegi e i permessi di accesso degli utenti identificati
- *Requisiti di immunità*
 - specificano come il sistema deve proteggersi da virus, worm e minacce simili



Categorie Requisiti di Sicurezza

- *Requisiti di integrità*
 - specificano come evitare la corruzione dei dati
- *Requisiti di scoperta delle intrusioni*
 - specificano quali meccanismi utilizzare per scoprire gli attacchi al Sistema
- *Requisiti di non-ripudiazione*
 - specificano che una parte interessata in una transazione non può negare il proprio coinvolgimento
- *Requisiti di riservatezza*
 - specificano come deve essere mantenuta la riservatezza delle informazioni



Categorie Requisiti di Sicurezza

- *Requisiti di controllo della protezione*
 - specificano come può essere controllato e verificato l'uso del sistema
- *Requisiti di protezione della manutenzione del sistema*
 - specificano come una applicazione può evitare modifiche autorizzate da un accidentale annullamento dei meccanismi di protezione



Villaggio Turistico

Requisiti di Sicurezza

- Creazione di un log per tracciare
 - tutte le azioni che avvengono sul sistema
 - i messaggi scambiati tra le parti del sistema
 - che vanno protetti in un qualche modo per evitare che un accesso fraudolento al sistema di log possa rivelare dati riservati
- Adottare meccanismi di analisi del log per
 - identificare pattern di accesso atipici
 - identificare discrepanze tra i messaggi spediti e ricevuti
- Individuare una corretta politica di controllo degli accessi
- I dati memorizzati e scambiati nel sistema devono essere protetti